https://doi.org/10.53587/25792865-2025.14-148

О ЦЕЛЕСООБРАЗНОСТИ НАЗНАЧЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ ПО УГОЛОВНЫМ ДЕЛАМ

Цветкова А.Д.

ФГБОУ ВО "Уральский государственный юридический университет имени В.Ф.Яковлева",
АНО "Центр содействия развитию криминалистики «КримЛиб»",
Екатеринбург, Россия

В статье анализируются критерии, которыми следует руководствоваться правоприменителю при решении вопроса о целесообразности назначения компьютерно-технической экспертизы по уголовным делам в условиях стремительного роста цифровизации. В качестве основных критериев рассматриваются: степень доступности компьютерной информации (открытая либо скрытая различными техническими средствами); её характер и тип (общедоступная и привычная пользователям либо специализированная, требующая профессиональных знаний); объём подлежащих исследованию данных (единичные цифровые объекты либо массивы больших данных); наличие и сложность использования необходимых технических средств; а также риск утраты криминалистически значимой информации при работе с цифровыми следами. Отдельное внимание уделяется неоднозначности влияния специфики совершённого преступления и доказательственного значения компьютерной информации на решение о назначении экспертизы, поскольку данные факторы не отражают уникальность конкретной следственной ситуации и могут создавать иллюзию алгоритмизации такого решения. Делается вывод о том, что комплексная и взвешенная оценка совокупности рисков и обстоятельств, связанных с исследованием цифровых следов, позволяет принимать сбалансированные решения, оптимизирующие нагрузку на экспертное сообщество и обеспечивающие высокое качество цифровых доказательств.

Ключевые слова: *компьютерно-техническая экспертиза, цифровые следы, криминалистический анализ, цифровизация, доказательственная информация, большие данные, уголовное судопроизводство, назначение экспертизы.*

Развитие современного общества неразрывно связано с феноменом цифровизации, которая проникает во все сферы жизнедеятельности. Данный процесс закономерно

Адрес для корреспонденции: Цветкова Анна Денисовна, младший научный сотрудник Центра содействия развитию криминалистики «КримЛиб» Уральского государственного юридического университета имени В.Ф.Яковлева, Россия, Екатеринбург,тел: +7 919 386 823, e-mail: ae@crimlib.info

отражается и на преступной активности: при совершении практически любого противоправного деяния в той или иной форме используются цифровые технологии. Злоумышленник может подбирать способ совершения преступления посредством поиска информации в сети Интернет, устанавливать контакт с соучастниками или потенциальными жертвами, в том числе в теневом сегменте сети (даркнете); приобретать орудия преступления или их составные части через онлайн-площадки с применением безналичных расчётов; с высокой долей вероятности попадать в поле стороннего видеонаблюдения, функционирующего в местах массового пребывания людей, и т.д. Помимо этого, существенно расширяется спектр компьютерных преступлений и деяний, совершаемых с использованием информационно-телекоммуникационных устройств.

Расширение роли цифровых технологий неизбежно приводит к формированию цифровых (компьютерных, электронных и др.) следов, исследование которых становится необходимым условием эффективного раскрытия и расследования преступлений любого вида.

Вместе с тем единообразного подхода к определению формы и пределов такого исследования не выработано. Наиболее значимая, на наш взгляд, сложность заключается в определении границы, за которой общих знаний следователя (дознавателя) или судьи становится недостаточно, и возникает необходимость привлечения специальных познаний посредством назначения профильной компьютерно-технической экспертизы. Представляется, что выработка универсального алгоритма действий правоприменителя в рассматриваемой сфере невозможна, поскольку криминалистические ситуации, складывающиеся по конкретным делам, нередко существенно различаются. Тем не менее представляется возможным сформулировать ориентировочные критерии, на которые следует опираться при принятии соответствующего процессуального решения.

Прежде всего необходимо учитывать степень **доступности самой информации**. Если для следствия интерес представляет переписка или иные данные, открыто хранящиеся в памяти электронного носителя, их изучение, как правило, не вызывает значительных затруднений и может быть осуществлено непосредственно правоприменителем, даже если для доступа приходится преодолевать парольную блокировку устройства. Иная ситуация возникает тогда, когда имеются основания полагать, что на пользовательском оборудовании содержится противоправный контент, но при поверхностном изучении он не обнаруживается. В подобных случаях целесообразно привлекать эксперта либо специалиста, обладающих компетенциями в области выявления криптографических и стеганографических закладок [1, стр. 198–200], посредством которых скрытая информация маскируется под внешне нейтральный материал (например, порнографическое изображение, встраиваемое во внутренние слои текстового документа).

Не менее значимым является критерий, связанный с **типом исследуемой информации**. При анализе текстовых файлов, фото-, видео- и аудиоматериалов, публикаций

в социальных сетях, сообщений в мессенджерах, веб-страниц в части их контентного содержания и иных данных, с которыми человек сталкивается ежедневно и которые стали естественным элементом современной цифровой среды как правило, специальные знания в области компьютерных технологий, не требуются. Однако в рамках подобных объектов могут потребоваться эксперты или специалисты из иных - не компьютерно-технических - областей: фоноскопии, речеведения, автороведения и др.

В то же время, вследствие преимущественно гуманитарной направленности образовательных программ в сфере юриспруденции, исследование «глубинных» слоёв цифровой информации требует специализированной технической квалификации. Несмотря на предпринимаемые попытки включения дисциплин по цифровой (компьютерной) криминалистике в учебные планы подготовки юристов [2], следователь, дознаватель или судья, как правило, не обладают достаточным уровнем навыков для самостоятельного получения и анализа, например, клавиатурного почерка, системных логов, метаданных различных файлов, либо установления признаков функционирования пользователя в теневом сегменте Интернет-сети. Следовательно, если формат цифровой информации является массовым и общеизвестным, её исследование может быть осуществлено правоприменителем непосредственно; в противном случае требуется назначение профильной компьютерно-технической экспертизы либо привлечение специалиста для консультации.

Не менее существенным представляется и **объём информации**, подлежащей исследованию. В тех случаях, когда следствию необходимо изучить отдельный акт переписки между двумя абонентами, конкретную веб-страницу, определённый документ либо единичный факт использования информационно-телекоммуникационных устройств, обращение к эксперту представляется избыточным. Это обусловлено отсутствием необходимости затрачивать значительные временные ресурсы, применять сложные аналитические подходы или специализированные технические средства для извлечения криминалистически значимой информации.

Иная ситуация возникает, когда требуется обнаружить неопределённый по содержанию или местоположению массив данных на пользовательском устройстве, обработать большие объёмы информации (например, данные о клавиатурном почерке), проанализировать сетевую активность за длительный временной период и т. п. В подобных случаях проведение экспертизы становится незаменимым. Это позволяет следователю (дознавателю) параллельно осуществлять иные следственные действия, пока эксперт проводит исследование, и обеспечивает гарантии корректного использования специализированных технических средств.

Особого внимания требует вопрос о выборе **технических средств**, необходимых для извлечения доказательственной информации. При решении вопроса о назначении компьютерно-технической экспертизы следует учитывать, какими именно устройствами и программными инструментами предполагается пользоваться, насколько ими владеет

правоприменитель, а также существует ли риск допущения ошибок, которые могут привести к порче или утрате криминалистически значимых данных. Если ответы на эти вопросы свидетельствуют о высокой технической сложности предстоящих действий, специфичности оборудования, отсутствии соответствующей подготовки у следователя (дознавателя) либо о возможности необратимой потери доказательственного материала вследствие неправильного применения средств обработки данных, экспертиза должна быть назначена.

В противоположность этому, если оборудование и методы его применения хорошо известны правоприменителю и не сопряжены с рисками искажений или утраты данных, их использование допускается без привлечения эксперта. При этом в каждом конкретном случае решение остаётся субъективно обусловленным - оно зависит от уровня компьютерной грамотности конкретного следователя (дознавателя) либо судьи: для одного специалиста восстановление удалённой информации или считывание содержимого жёсткого диска не представляет трудности, тогда как для другого затруднительным может оказаться даже определение исполнителя электронного документа или даты его последнего изменения.

Ещё одним критерием, сформировавшимся в практической деятельности, является **специфика совершённого преступления** и характер цифровых следов. В литературе высказывается мнение, что компьютерно-техническая экспертиза должна назначаться при расследовании преступлений, диспозиции которых прямо предусматривают использование информационно-телекоммуникационных сетей, либо преступлений, отнесённых к сфере компьютерной информации [3, стр. 120]. Однако данный подход вряд ли можно считать универсальным, поскольку он не учитывает конкретную следственную ситуацию. Так, хотя УК РФ предусматривает квалифицирующий признак клеветы, связанный с распространением порочащих сведений через информационно-телекоммуникационные сети (например, посредством публикации в социальной сети), для установления самого факта размещения записи привлечение эксперта-компьютерщика не требуется; напротив, может потребоваться участие специалиста-речеведа, если высказывание имеет завуалированный характер.

В то же время при расследовании незаконного оборота оружия преступная деятельность может быть связана с использованием даркнета, где установление обстоятельств заключения преступной сделки без специальных знаний значительно затруднительно. Следовательно, ориентироваться исключительно на диспозицию уголовно-правовой нормы при решении вопроса о необходимости назначения компьютерно-технической экспертизы неправильно. Определяющее значение должны иметь обстоятельства, связанные с объёмом и доступностью информации, уровнем технической сложности её получения и рисками утраты доказательственных сведений.

Ещё одним критерием, к которому следует подходить с особой осторожностью, является **потенциальная доказательственная роль компьютерной информации**. На практике нередко складывается ситуация, когда заключение эксперта приобретает повышенное значение вследствие исключительной компетентности специалиста,

проводившего исследование. Психологически человек склонен безоговорочно доверять мнению профессионала в соответствующей области. В результате, несмотря на формально равную юридическую силу всех доказательств, протокол осмотра электронного носителя информации и заключение компьютерно-технической экспертизы воспринимаются правоприменителем неодинаково, и приоритет зачастую отдаётся последнему.

С одной стороны, это использование экспертного потенциала может укрепить позицию одной из сторон: если компьютерная информация предполагается в качестве основного доказательства по делу, более перспективным представляется её исследование экспертом. С другой стороны, важно не поддаться иллюзии технологической «автоматизации» [4, с. 206] и не подменять ответственность правоприменителя мнением эксперта, фактически смещая центр принятия процессуальных решений.

Наконец, последним критерием, которому следует уделить отдельное внимание, является **риск утраты доказательственной информации**. Он уже упоминался в контексте предыдущих факторов, однако его значение столь существенно, что позволяет рассматривать его как один из ключевых при принятии решения о необходимости назначения экспертизы.

Цель криминалистической деятельности - установление всех обстоятельств совершённого преступления, включая личность виновного. Это возможно лишь при условии всестороннего изучения релевантной информации. Итогом должен стать целостный, логически непротиворечивый образ события преступления и его участников, ясный как для правоприменителя, так и для суда. Достижение такой ясности обеспечивается путём формирования непрерывной системы доказательств, полученных из разнообразных криминалистически значимых источников. Поэтому сохранность информационных следов и производных доказательств является необходимым условием успешного раскрытия и расследования преступлений.

Исходя из этого, если правоприменитель осознаёт, что его компетенций недостаточно для самостоятельного исследования цифровых следов с обеспечением их сохранности, то с точки зрения минимизации рисков необоснованного привлечения к ответственности либо оправдания виновного целесообразно назначить компьютерно-техническую экспертизу. Эксперт располагает специализированным оборудованием, обладает глубокими знаниями о возможных рисках при работе с цифровой информацией и способен обеспечить её защиту в большей степени, чем следователь (дознаватель) или судья.

Вместе с тем подчеркнём: изложенное не означает необходимости направления на экспертизу всех без исключения электронных носителей информации. Такая практика привела бы к неоправданному увеличению нагрузки на экспертные учреждения, что, в свою очередь, чревато затягиванием сроков предварительного расследования и снижением качества отдельных исследований. Следовательно, каждый акт оценки рисков утраты криминалистически значимой информации должен представлять собой ответственное, взвешенное и рациональное решение.

На наш взгляд, ориентация правоприменителя на предложенные критерии и соблюдение разумного баланса при использовании специальных познаний позволит снизить избыточную экспертную нагрузку, повысить качество сложных исследований, оптимизировать сроки расследования и одновременно обеспечить представление квалифицированных доказательств именно в тех случаях, когда в них действительно имеется необходимость.

Информация о финансировании:

Исследование выполнено при финансовой поддержке гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/.

Список литературы:

1. Смахтин Е. В., Льянов М. М. Сокрытие электронно-цифровых следов как способ противодействия расследованию преступлений // Технологии XXI века в юриспруденции: Материалы Пятой международной научно-практической конференции, Екатеринбург, 19 мая 2023 года. Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб»», 2023. С. 195–203.
2. Абламейко М. С. Криминалистическое компьютероведение как новая дисциплина для подготовки специалистов для расследования преступлении в сфере высоких технологии // Судебная экспертиза Беларуси. 2020. № 1 (10). С. 32–36.
3. Соколов А. Б., Сысенко А. Р. Назначение и производство компьютерной экспертизы при расследовании преступлений, совершенных с использованием сети Интернет: проблемы теории и практики // Криминалистика: вчера, сегодня, завтра. 2021. № 1 (17). С. 118–129. DOI 10.24412/2587-9820-2021-1-118-129.
4. Бахтеев Д. В. Теория криминалистического мышления: монография. Москва: Издательство «Юрлитинформ», 2024. 264 с.

ՀԱՄԱԿԱՐԳՉՏԵԽՆԻԿԱԿԱՆ ՓՈՐՁԱՔՆՆՈՒԹՅՈՒՆՆԵՐԻ ՆՇԱՆԱԿՄԱՆ ՆՊԱՏԱԿԱՀԱՐՄԱՐՈՒԹՅՈՒՆԸ ՔՐԵԱԿԱՆ ԳՈՐԾԵՐՈՒՄ

Յվեփկովա Ա.Դ.

Հոդվածում վերլուծվում են այն չափանիշները, որոնցով պետք է առաջնորդվի իրավակիրառողը՝ քրեական գործերով համակարգչատեխնիկական փորձաքննություն նշանակելու նպատակահարմարության վերաբերյալ հարցի քննարկման ժամանակ՝ թվայնացման ներկայիս աճի պայմաններում: Որպես հիմնական չափանիշներ դիտարկվում են համակարգչային տեղեկատվության հասանելիության աստիճանը (բաց կամ տարբեր տեխնիկական միջոցներով թաքցված), դրա բնույթը և տեսակը (հանրամատչելի և օգտատիրոջ համար սովորական կամ մասնագիտացված, որը պահանջում է մասնագիտական գիտելիքներ), ուսումնասիրության ենթակա տվյալների ծավալը (մեկական

թվային օբյեկտներ կամ մեծածավալ տվյալների զանգվածներ), անհրաժեշտ տեխնիկական միջոցների առկայությունը և դրանց օգտագործման բարդությունը, ինչպես նաև թվային հետքերի հետ աշխատանքի ընթացքում քրեական նշանակություն ունեցող տեղեկատվության կորստի ռիսկը: Առանձին ուշադրություն է դարձվում կատարված հանցագործության առանձնահատկությունների և համակարգչային տեղեկատվության ապացուցողական նշանակության ազդեցության ոչ միանշանակ լինելուն՝ փորձաքննություն նշանակելու վերաբերյալ որոշման ընդունման ընթացքում, քանի որ նշված գործոնները չեն արտացոլում կոնկրետ քննչական իրավիճակի յուրահատկությունը և կարող են սպեղծել նման որոշման ալգորիթմայնացման պատրանք: Եզրակացվում է, որ թվային հետքերի ուսումնասիրման հետ կապված ռիսկերի և հանգամանքների ամբողջության համալիր և կշռադատված գնահատումը հնարավորություն է տալիս ընդունել հավասարակշռված որոշումներ, որոնք օպտիմալացնում են փորձագիտական համայնքի ծանրաբեռնվածությունը և ապահովում թվային ապացույցների բարձր որակը:

Բանալի բառեր. *համակարգչատեխնիկական փորձաքննություն, թվային հետքեր, քրեական վերլուծություն, թվայնացում, ապացուցողական տեղեկատվություն, մեծ տվյալներ, քրեական դատավարություն, փորձաքննության նշանակումը:*

ON THE EXPEDIENCY OF APPOINTING COMPUTER-TECHNICAL EXAMINATIONS IN CRIMINAL CASES

Tsvetkova A.

The article analyzes the criteria that should guide law-enforcement practitioners when deciding on the expediency of appointing a computer-technical examination in criminal cases amid the rapid growth of digitalization. The main criteria considered are: the degree of accessibility of computer information (open or concealed by various technical means); its nature and type (publicly accessible and familiar to users or specialized, requiring professional knowledge); the volume of data to be examined (individual digital objects or large data arrays); the availability and complexity of using the necessary technical tools; as well as the risk of losing forensically significant information when working with digital traces. Particular attention is paid to the ambiguous impact of the specifics of the committed crime and the evidentiary value of computer information on the decision to appoint an examination, since these factors do not reflect the uniqueness of a particular investigative situation and may create the illusion of algorithmizing such a decision. It is concluded that a comprehensive and balanced assessment of the totality of risks and circumstances associated with the examination of digital traces makes it possible to make well-grounded decisions that optimize the workload of the expert community and ensure the high quality of digital evidence.

Keywords: *computer-technical examination, digital traces, forensic analysis, digitalization, evidentiary information, big data, criminal proceedings, appointment of an examination.*

Ներկայացվել է խմբագրության 14.09.2024
Ընդունվել է տպագրութան 01.07.2025